Securing Our Homeland, Strengthening Our Liberties

Prepared by the Democratic Members of the
House Select Committee on Homeland Security
Jim Turner, Ranking Member

228 Adams Building
101 Independence Avenue, SE
Washington, DC 20540
202-226-2616
http://www.house.gov/hsc/democrats/

DEMOCRATIC MEMBERS OF THE HOUSE SELECT COMMITTEE ON HOMELAND SECURITY

Jim Turner, Texas
Ranking Member

Bennie G. Thompson, Mississippi
Ranking Member, Subcommittee on Emergency Preparedness and Response

Loretta T. Sanchez, California
Ranking Member, Subcommittee on Infrastructure and Border Security

Louise M. Slaughter, New York
Ranking Member, Subcommittee on Rules

Zoe Lofgren, California
Ranking Member, Subcommittee on Cybersecurity, Science, and Research & Development

Karen McCarthy, Missouri
Ranking Member, Subcommittee on Intelligence and Counterterrorism

Edward J. Markey, Massachusetts

Norman D. Dicks, Washington

Barney Frank, Massachusetts

Jane Harman, California

Benjamin L. Cardin, Maryland

Peter A. DeFazio, Oregon

Nita M. Lowey, New York

Robert E. Andrews, New Jersey

Eleanor Holmes Norton, District of Columbia

Sheila Jackson-Lee, Texas

Bill Pascrell, Jr., New Jersey

Donna M. Christensen, U.S. Virgin Islands

Bob Etheridge, North Carolina

Ken Lucas, Kentucky

James R. Langevin, Rhode Island

Kendrick B. Meek, Florida

Ben Chandler, Kentucky

Table of Contents

~

Securing Our Homeland, Strengthening Our Liberties

The national effort to protect our homeland focuses on preserving the "unalienable rights that are essential to the strength and security of our nation: life, liberty, and the pursuit of happiness."[1] Thus, if developed properly, our homeland security efforts should reinforce the civil liberties and values that make America strong.[2]

The challenge, however, is to develop homeland security initiatives that are consistent with our society's constitutional guarantees relating to privacy, due process, and civil liberties. As our government develops post 9/11 homeland security initiatives in areas such as immigration, intelligence collection, law enforcement, and the use of new technologies it must thoughtfully and carefully review their impact on our fundamental freedoms. To conduct such a review requires both leadership and an evaluative framework to guide the government.

For example, if there is not adequate leadership within the government to guide privacy policy, there may be unnecessary impositions on the freedoms and privileges enjoyed in the United States. Likewise, homeland security could suffer if needed initiatives do not gain public support due to meritorious concerns about privacy protections. As the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, also known as the Gilmore Commission ("Gilmore Commission"), found last December "[g]overnments must look ahead at the unintended consequences of policies in the quiet of the day instead of the crisis of the moment."[3]

Federal Government Privacy: Leadership and Accountability Is Lacking

In February 2003, the General Accounting Office (GAO) released a report finding that the Administration was not providing sufficient leadership, oversight, and guidance on privacy issues, in particular, the Privacy Act.[4] The assessment was based on feedback from twenty-four different agency representatives who said that, in addition to gaps in guidance from the Office of Management and Budget, agencies were not prioritizing the need to comply with the Privacy Act and were not providing sufficient employee training on the Act. The GAO stated that if these issues were not addressed, the "government will not be able to provide the public with sufficient assurance that all legislated individual privacy rights are adequately protected."[5]

The federal government's failure to adequately protect individual privacy rights, especially those required by law, may be due in part to the deprioritization of privacy within the Executive

---

[1] Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, also known as the Gilmore Commission, "Forging America's New Normalcy: Securing Our Homeland, Protecting Our Liberty," December 2003, http://www.rand.org/nsrd/terrpanel/volume_v/volume_v_report_only.pdf.

[2] Ibid.

[3] Ibid.

[4] General Accounting Office, Privacy Act: OMB Leadership Needed to Improve Agency Compliance, GAO-03-304, June 2003.

[5] Ibid.

Branch. In 1998, President Clinton required every agency to "designate a senior official within the agency to assume primary responsibility for privacy policy."[6] The next year, the President created a "chief counselor for privacy" position for the federal government within the Office of Management and Budget to advise on privacy issues. The counselor reviewed proposals before they went public and when there were privacy problems fixed them before the proposals were implemented.[7]

The privacy counselor position was eliminated, however, at the beginning of the current Administration. This occurred despite the urging of many in the private sector, academia, and the government to fill the position.[8] In addition, many of the senior officials assigned to handle privacy policy within the federal agencies left the government and were never replaced.[9] Thus, there is no senior official within the White House or Office of Management and Budget leading the effort to secure our homeland by strengthening our citizen's liberties and privacy. No one is providing meaningful leadership in either of these offices to evaluate privacy in new technologies throughout the federal government.

Recognizing the need to have someone responsible for privacy relating to homeland security programs, Congress required the Department of Homeland Security to create a "privacy office," tasking it with the following:

- Ensuring that Department of Homeland Security complies with the Privacy Act of 1974;
- Adequately considering privacy when Department of Homeland Security collects, uses, and discloses personal information; and
- Properly assessing the impact of its practices and rules on privacy.[10]

The privacy office, however, is only responsible for evaluating the privacy of programs within Department of Homeland Security. Many of the technologies, information sharing, and gathering mechanisms relating to homeland security are being implemented by the Administration in agencies other than Department of Homeland Security. The result is that there is no comprehensive and uniform evaluation of homeland security privacy issues in the federal government, especially in light of the elimination of the privacy counselor position within the White House. Without a single, accountable senior official to ensure that homeland security programs are evaluated in a uniform manner, our nation's privacy and civil liberties are at risk.

---

[6] William J. Clinton, "Memorandum for the Heads of Executive Departments and Agencies," May 14, 1998, http://www.cdt.org/privacy/survey/presmemo.html.

[7] William Matthews, "Privacy Czar Plays Homeland Role," *Federal Computer Week*, November 21, 2002, http://www.fcw.com/fcw/articles/2002/1118/web-private-11-21-02.asp.

[8] Letter to Mitch Daniels, Director, Office of Management and Budget, April 16, 2001, http://www.cdt.org/privacy/010416omb.shtml.

[9] Statement of James X. Dempsey, House Committee on the Judiciary, Subcommittee on Commercial and Administrative Law, "Privacy in the Hands of the Government: The Privacy Officer for the Department of Homeland Security."

[10] Roy Mark, "Homeland Security Names First Privacy Czar," *dc.internet.com,* April 17, 2003, http://dc.internet.com/news/article.php/2192521.

RECOMMENDATION

The Administration should move promptly to name a senior level official to be responsible for government-wide leadership on privacy issues. In recent congressional hearings, several privacy experts stated that our country needs a chief privacy officer at OMB who could advise agencies on federal privacy policies and direct government-wide policies, where needed.[11] *As noted by Sally Katzen, a University of Michigan Law School professor and former Office of Management and Budget official, "an office inside [the Office of Management and Budget] can provide institutional memory and sensitivity ... At the least, the appointment of a highly qualified privacy guru ... would mean that someone in a senior position, with visibility, would be thinking about these issues before – rather than after – policies are announced."*[12]

In addition to a government-wide chief privacy officer, the federal government should reinstate senior privacy officers within each of the federal agencies to ensure that each of those agencies is accountable in its handling of privacy matters. The Homeland Security Act's creation of a privacy office within the Department of Homeland Security can serve as model for how other agencies can structure their privacy duties. In particular, each agency should focus on privacy protections relating to the collection, use, and distribution of personally-identifiable information, ensuring that personally-identifiable information is adequately protected while in the government's possession, and conducting privacy impact assessments on programs and policies within the each.

Technology, Privacy, and Civil Liberties: "Privacy by Design"

In recent years, technology has advanced significantly, with the advent of biometrics, supercomputing, interconnected global networks, the Internet, and other new technologies. These technologies, along with improved information sharing and collection systems, are critical tools in the battle to secure our homeland and win the war on terror. Emerging technologies give federal agencies the capability to access and analyze large amounts of information in a cohesive manner, regardless of whether that information is held in databases and networks at different agencies, thereby increasing the likelihood that we can identify potential terrorists.

Technology also gives federal agencies the capability to access homeland security information. In doing so, however, the government must ensure that information is accurate, remains confidential, and that access is limited to only appropriate personnel so as to protect civil liberties and privacy. Given the sensitivity of information gathered about individuals, it is also imperative that this data be protected during its creation, transmission, and storage.[13]

---

[11] Sara Michael, *Officials Call for Privacy Czar*, fcw.com, February 11, 2004.

[12] Testimony of Sally Katzen, "Privacy in the Hands of the Government: The Privacy Officer for the Department of Homeland Security," The Committee on the Judiciary, Subcommittee on Commercial and Administrative Law, February 10, 2004.

[13] Markle Foundation's Task Force on National Security in the Information Age, "Protecting America's Freedom in the Information Age," October 2002, and "Creating a Trusted Network for Homeland Security," December 2003.

Likewise, if the government uses information that is held by the private sector, it must do so within a system of rules and guidelines that protect civil liberties. In today's technology-dependent, transaction-friendly society, Americans produce millions of records of their daily activities – ranging from credit card purchases to government registration and accounting systems to logs of personal time spent on the Internet and in entertainment venues. Unchecked access to such information by the government and other entities without sufficient cause could violate many of our constitutional rights.

As noted in a bipartisan proposal developed by former government officials from the Clinton and Reagan administrations, for our government to properly protect our citizenry's privacy it must take into account "the revolutionary changes in recent years in communication, surveillance and database technology, and the implications of those changes for individual privacy and personal liberties."[14] Unfortunately, the federal government has not conducted a comprehensive assessment of the use of new technologies and privacy in 30 years. The original Privacy Act of 1974 established the "U.S. Privacy Protection Study Commission" to evaluate the statute and issue a report on how to improve privacy protections. The Commission issued its report "Personal Privacy in an Information Society" in 1977 and ceased its operations. Since that time, there has not been a comprehensive national government-wide effort to evaluate the privacy implications of new technologies.

As a result, the government's efforts successfully to use technology while also protecting privacy and civil liberties are lagging. In reports issued in 2002 and 2003, the Markle Foundation's Task Force on National Security in the Information Age found that the government lacked a "systematic effort to consider the privacy implications of the proposed programs or to develop an overall policy framework that would govern the deployment of new technologies."[15] To protect civil liberties, the Task Force stated that our country needs a framework that the government can use to secure new technologies and develop privacy-protecting processes. To effectively combat terrorism and protect privacy, a framework establishing clear policies and guidelines is needed to "identify the types of databases involved, define the purposes of the data review, and clarify the authorization for collecting and disseminating whatever is found."[16] Such a framework could assist the government's homeland security efforts, allowing it to use technology to better manage and sort the large amount of data it gathers.

A framework also can help us ensure that databases used across the government operate within federal privacy laws and do not offend our constitutional values. Protecting our homeland and protecting our citizen's privacy should not be a "balancing act" where one is sacrificed for the benefit of the other. Rather, homeland security and privacy should reinforce one another through safeguards that build oversight and restraints on the misuse of power into our security initiatives.

---

[14] Peter Swire and Jeffrey Eisenach , "Ensuring privacy's post-attack survival," *Zdnet.com*, September 11, 2002, http://zdnet.com.com/2100-1107-957464.html.

[15] Markle Foundation's Task Force on National Security in the Information Age, "Protecting America's Freedom in the Information Age," October 2002, and "Creating a Trusted Network for Homeland Security," December 2003.

[16] Ibid.

In a recent congressional hearing, Jim Dempsey, the Executive Director of the Center of Democracy and Technology, stated the government must be able to conduct "privacy by design."[17] More specifically, he stated:

> One of the best ways to protect privacy, while facilitating the effective collection and use of information where necessary to carry out a governmental function, is to raise privacy concerns early in the development of a new program, so that those concerns can be addressed and mitigated in advance.[18]

In the past year, several homeland security initiatives have been derailed or postponed because the Administration has failed to adequately evaluate the programs' effects on privacy and civil liberties. These events make it all to clear that the federal government lacks a "privacy by design" plan. There are no consistent mechanisms or safeguards to ensure that homeland security initiatives fortify not only our physical security, but also the security of our constitutional rights.

The problems associated with the Terrorism (first known as Total) Information Awareness (TIA) project, an initiative within the Defense Advanced Research Project Agency's Information Awareness Office, serves as an example of what can happen when proposals are launched without fully considering their impact on individual privacy. The program was designed to analyze as much information as possible on individuals and use computers and human analysis to detect potential terrorist activity. It planned to search existing databases containing information such as financial records, medical records, communication records, and travel records to find matches for particular patterns.[19] Concerns regarding civil liberties and privacy led to Congress eliminating the Information Awareness Office responsible for creating the program.

Concerns also have been raised by the Computer Assisted Passenger Prescreening System (CAPPS) II, which uses databases to check airline passengers' backgrounds and scores passengers on their potential to be a terrorist risk. Various civil liberties and privacy issues have been identified with CAPPS II, including the lack of safeguards in place to protect passengers wrongly identified as terrorists, as well as questions regarding whether adequate security protections are in place to keep hackers and other criminals from accessing the personal information of passengers. As a result, Congress mandated that the program not be deployed until the General Accounting Office (GAO) completed a privacy and civil liberties assessment of the program.[20] The GAO report was inconclusive on TSA's privacy efforts. The report found that "[u]ntil TSA completes its privacy plans and the program is further developed," it could not be determined if the agency had identified all of the privacy risks and necessary mitigation efforts.[21]

Not only does the government lack a framework in which to evaluate emerging technologies, it does not have in place a uniform system for the collection, use, and data from private sector databases and lists. The lack of uniformity has resulted in several widely-reported incidents

---

[17] Testimony of Jim Dempsey, "Privacy in the Hands of the Government: The Privacy Officer for the Department of Homeland Security," The Committee on the Judiciary, Subcommittee on Commercial and Administrative Law, February 10, 2004.

[18] Ibid.

[19] Report to Congress regarding the Terrorism Information Awareness Program, May 20, 2003, http://www.darpa.mil/body/tia/tia_report_page.htm

[20] Judi Hasson, "Congress Demands Study of CAPPS II," *fcw.com*, September 26, 2003, http://www.fcw.com/fcw/articles/2003/0922/web-capps-09-26-03.asp.

[21] Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges, General Accounting Office, GAO-04-385, February 2004.

where personally identifiable information has been turned over to the federal government or contractors without adequate controls and processes. For example, three airlines have all come forward in the past year to admit that they turned over massive amounts of passenger itineraries to the government. Specifically:

- In September 2003 JetBlue admitted that it had given five million passenger itineraries, possibly through the assistance of the Transportation Security Agency (TSA), to a defense contractor as part of a study seeking ways to identify high risk customers.[22]

- In January, Northwest Airlines admitted that it handed over three months of passenger records to the National Aeronautics and Space Administration in 2001 for a data mining project.

- Last month, American Airlines – the world's largest airline said that it gave approximately 1.2 million passenger itineraries to the Transportation Security Administration, as well as several research companies vying for contracts with the agency in 2002.[23]

These disclosures were done without notification to customers, almost all of whom are presumably law-abiding individuals with no connections to terrorists. Consequently, several federal agencies are investigating the disclosures and class action lawsuits have been filed against all three airlines for potential privacy violations.[24]

The result of the government's shortcomings in building strong privacy programs is that some potentially useful information-sharing projects and mechanisms have not come to fruition. Many of these might have been successfully implemented if civil liberties and privacy had been given great attention during their development. Benjamin Franklin once said "they that would give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." Our government must strive to be better in its implementation of new programs to protect our homeland, as Americans deserve both their liberty and safety.

RECOMMENDATION

In order to ensure that a comprehensive privacy and homeland security evaluation is completed, the Administration should create a new Commission on Privacy, Freedom, and Homeland Security.[25] This Commission should be responsible for conducting a comprehensive legal and factual study on the United States efforts to further homeland security in a manner that protects privacy, civil liberties, and individual freedoms. The Commission should be charged with drafting findings and recommendations on, among other items, how agencies are

---

[22] Thomas Claburn, "Northwest CEO Urges Airline Execs To Talk Privacy," *Information Week*, January 22, 2004, http://www.informationweek.com/story/showArticle.jhtml?articleID=17500687.

[23] "American Released Privacy Data," wired.com, April 10, 2004, http://www.wired.com/news/privacy/0,1848,63018,00.html?tw=wn_tophead_3.

[24] Ryan Singel, "Army Quietly Opens JetBlue Probe," *Wired*, November 26, 2003, http://www.wired.com/news/privacy/0,1848,61374,00.html.

[25] Peter Swire and Jeffrey Eisenach , "Ensuring privacy's post-attack survival," *Zdnet.com*, September 11, 2002, http://zdnet.com.com/2100-1107-957464.html.

and should be assessing the privacy implications of new homeland security technologies before implementing them and deploying them. The Commission also should review and make recommendations on procedures for the federal government's use of individual personal information from commercial databases and lists.
